HOW TO SURVIVE THE MS-DOS CHKDSK BUG

ARE YOU AT RISK?

You may be at risk if you are using MS or PC-DOS 4.00 or 4.01 or 5.0 and your hard disk exceeds 127 Mbyte

(For full details see text)

Some version of CHKDSK may cause you to lose all the data on your disk. A bug within this external command in MS-DOS and PC-DOS 4.0, 4.1 and 5.0 can cause the total loss of your directory structure and data in a few seconds – if your configuration is one of those at risk.

COULD YOU BE IN JEOPARDY?

CHKDSK is used to report on the basic integrity of the FAT (File Allocation Table), a short map of all the parts on your disk where programs and data are stored. If the /F switch is included with the command, it will not only report errors (lost clusters) but will give an opportunity to make new files out of each unconnected chain of clusters, or alternatively release them back to the pool of unused clusters. Lost clusters are a commonplace problem within a FAT – quite often the result not of corruption but of using Ctrl-Alt-Del when a test program has gone wrong.

If you use CHKDSK /F on a disk partition with a FAT 256 sectors long and elect to return lost chains to the pool (by answering 'N' to the question 'Convert lost chains to files?'), the bug in CHKDSK will write 256 copies of your FAT onto the disk – overwriting your entire directory structure.

There is a simple way to tell if you are immediately at risk: for each disk partition (that is, device letter which is on the hard disk) enter CHKDSK without the /F switch. You will get a display that looks like this, but with different numbers:

```
Volume Serial Number is 3D13-12F9

 244834304 bytes total disk space
  1671936 bytes in 9 hidden files
  1449984 bytes in 346 directories
182697984 bytes in 6939 user files
 39014400 bytes available on disk

     4096 bytes in each allocation unit
    59774 total allocation units on disk
     9525 available allocation units on disk
```

The number listed as 'total allocation units on disk' is the crucial indicator: if it is greater than 65278, you are at risk! This number will not change unless you subsequently run the FDISK program to change the partition size.

Microsoft has mentioned this problem in a partial manner in their Knowledge Base – an open database of hints, tips and bugs found in their products. (You can see this database on CompuServe – GO MSKB). In an article entitled 'When Not to Use MS-DOS 5.0 CHKDSK and UNDELETE Commands' users are warned that when used on disk partitions with a FAT of the crucial size, the CHKDSK /F option 'will harm such drives' and the UNDELETE 'will be unpredictable'.

This document doesn't spell out the extent of the bug, but gave sufficient details so that Alan Solomon's team at S&S International confirmed the details we have given; they also found that the following versions of the CHKDSK program have the bug.

Operating System	File	Size	Dated
PC-DOS 4.01	CHKDSK.COM	17771	17 Jun 88
MS-DOS 4.01	CHKDSK.COM	17787	30 Nov 88
MS-DOS 5.0	CHKDSK.EXE	16200	09 Apr 91
PC-DOS 5.0	CHKDSK.COM	16184	09 May 91

The Knowledge Base goes on to say that the error was corrected in maintenance release 5.0A, and that the corrected versions of CHKDSK.EXE and UNDELETE.EXE are dated 11 November 91.

If all your hard disks are less than 128 Mbyte in size and you know for sure you will not get new equipment before MS-DOS 6.0 is released next year, then you can rest assured.

If you are using DR DOS 6.0, Novell NetWare or Unix you are also safe from this problem. If instead of CHKDSK you use Norton Disk Doctor to do FAT repairs, you are safe.

Otherwise, we suggest you contact Microsoft on its support number, (0734) 270000, and quote document number Q80496 from its Knowledge Base: maybe the company will decide that you are entitled to the maintenance release.

Your first step, we suggest, is to make sure CHKDSK is not executed from within your AUTOEXEC.BAT (a common strategy). It may be a good idea to rename your faulty CHKDSK.EXE so that any other user of your system will not innocently activate the bug. ●

FAT CHANGES

Both floppy and hard disks have a FAT (File Allocation Table), consisting of many entries, each representing a cluster on the disk. On a hard disk in the days before MS-DOS 4.0 each cluster was 2K long. Each file started at a cluster boundary, and so the amount of space it occupied on disk was always an even number of kilobytes. The largest possible FAT occupied 64 sectors, giving a maximum partition size of 32 Mbyte using 2-byte cluster tags.

MS-DOS version 4.0 introduced a new technology for handling very large disk partitions: the disk cluster became 4K long, and so the FAT could be much smaller. For a partition of 129 Mbyte, only 128 sectors were required; the full 256-sector FAT could represent 256 Mbytes. If 257 Mbytes were needed, the cluster size expanded to eight sectors, and the new FAT would shrink again to 128 sectors.

The CHKDSK bug occurs when the FAT is at its largest possible size – 256 sectors. This coincides with partition sizes of 128 Mbyte, 256 Mbyte, 512 Mbyte and 1,024 Mbyte – but it is easier to note the 'total allocation units on disk' being larger than 65,278, which comes down to the same thing.

WHAT'S ON A HARD DISK

The contents of a hard disk formatted for use with MS-DOS is listed below as follows:

1. A partition record; this defines the location and length of each of the partitions of a disk. A disk may have one or more partitions – each functioning as a disk 'device'.

2. Partitions, made up as follows..

(a) The 'active DOS' partition has a BOOT sector, containing start-up code that executes during a warm or cold boot; it locates the BIOS and DOS hidden files, starts the process of loading drivers (from CONFIG.SYS), and finally hands control to DOS to load COMMAND.COM and process AUTOEXEC.BAT.

(b) The FAT for the partition, plus one copy

(c) The directory structure for the partition

(d) The data area for the partition

The CHKDSK bug is particularly destructive because it writes hundreds of extra copies of the FAT: these write 32 Mbyte of redundant information over the partition's directory structure, and potentially over a great deal of : all filenames are lost, and even a data recovery service will have trouble retrieving much.